

Biometric E-Commerce: Security in B2C (Business-to-Consumer)

By

Goh Kim Nee

Dissertation submitted in partial fulfillment of
the requirements for the
Bachelor of Technology (Hons)
(Information Technology)

JUNE 2004

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

t

HF

5548.72

5614

2004

1) Electronic commerce -- security measures

2) Business enterprises -- Computer networks -- Security measures

3) IT/IS -- Trends

CERTIFICATION OF APPROVAL

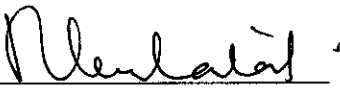
Biometric E-Commerce: Security in B2C (Business-to-Consumer)

By

Goh Kim Nee

A project dissertation submitted to the
Information Technology Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirements for the
BACHELOR OF TECHNOLOGY (Hons)
(INFORMATION TECHNOLOGY)

Approved by,

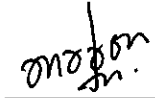

(Mr. Khairul Shafee Kalid)

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK

June 2004

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



(GOH KIM NEE)

ABSTRACT

Every e-commerce transaction done online seemed to be a secure transaction. However, many users do not realize the fraud that happens while doing transactions. Of course, there are ways to curd this rising problem. The objective of this project is to study the feasibility and the security of e-commerce by implementing fingerprint biometric during transaction. The key point is to create a safe and secure environment for users to do transactions on the Internet without the need to worry about fraud. The methodology used will be Retotype, a combination of research and prototype. A Retotype will be modeled to capture the most efficient and secure e-commerce transaction method. The final product would be a prototype of an e-commerce website incorporated with fingerprint biometric as an authentication method. An implementation strategy would be analyzed to weigh how practical can this system work in the real world.

ACKNOWLEDGEMENT

This project would not be completed if there were not any support and guidance from the wiser ones. I would like to take this opportunity to thank certain people who made it all happen.

Firstly, I would like to thank God for giving me the strength, wisdom and guidance to complete this project. Secondly, I would like to thank my supervisor, Mr. Khairul Shafee Kalid who never failed to give support, advices and suggestions into making this project a great and successful one.

I would like to also thank Mr. Foong Wai Seng for his constructive comments that open my mind into enhancing this project.

Lastly I would like to thank my friends and family members for supporting me, understanding, helping and guiding me through. Without them, I would be incomplete.

Once again, a big thank you. God bless.

TABLE OF CONTENTS

CERTIFICATION OF APPROVAL	ii
CERTIFICATION OF ORIGINALITY	iii
ABSTRACT	iv
ACKNOWLEDGEMENT	v
LIST OF FIGURES	viii
ABBREAVIATIONS AND NOMENCLATURES	ix

CHAPTER 1 – INTRODUCTION

1.1 BACKGROUND OF STUDY	1
1.2 PROBLEM STATEMENT	1
1.3 OBJECTIVES AND SCOPE OF STUDY.....	3
1.3.1 Objectives	3
1.3.2 Scope of Study	3

CHAPTER 2 – LITERATURE REVIEW AND THEORY

2.1 THE E-COMMERCE PROCESS	5
2.2 NUMBER ONE FRAUD IN E-COMMERCE	6
2.3 EFFECTS OF IDENTITY THEFT OR CREDIT CARD FRAUD	7
2.4 DISADVANTAGES OF PASSWORD AUTHENTICATION	8
2.5 BIOMETRIC AND WHAT IT DOES	8
2.6 BIOMETRIC E-COMMERCE	9
2.7 BIOMTERICS ROLE IN SOLVING IDENTITY THEFT AND FRAUD.....	10
2.8 PREVIOUS ONLINE BIOMETRIC WORKS	11
2.8.1 Using Biometric For Authenticating Online Exam Students	11
2.8.2 Biometric E-Commerce	11

CHAPTER 3 - METHODOLOGY / PROJECT WORK

3.1 PROCEDURE IDENTIFICATION..... 13

3.1.1 Problem Identification And Solution Work 13

3.1.2 Research And Feasibility Study..... 14

3.1.3 Design 14

3.1.4 Build prototype/ model 14

3.2 TOOLS REQUIRED..... 15

3.2.1 Hardware..... 15

3.2.2 Software..... 15

CHAPTER 4 - RESULTS AND DISCUSSION

4.1 ARCHITECTURE OF BIOMETRIC E-COMMERCE..... 16

4.2 BIOKEY ARCHITECTURE..... 17

4.3 STAGES IN THIS SYSTEM..... 19

4.3.1 The ‘BEFORE’ Stage..... 19

4.3.2 The ‘DURING’ Stage..... 25

4.3.3 Wisdom Bookstore Website..... 26

4.3.4 The ‘AFTER’ Stage..... 33

4.4 IMPLEMENTATION ISSUES..... 33

4.4.1 Implementation of biometric e-commerce..... 33

4.4.2 Usage of biometric..... 34

4.5 LIMITATIONS OF THE SYSTEM..... 35

4.5.1 Change of Credit Card Number..... 35

4.5.2 Security at server side..... 35

4.6 FUTURE ENHANCEMENT..... 35

4.6.1 Scar finger..... 35

4.6.2 Multiple credit cards..... 36

4.6.3 Change of credit card number..... 36

CHAPTER 5 – CONCLUSION..... 37

REFERENCES..... 38

LIST OF FIGURES

Figure 1: The e-commerce process.....	5
Figure 2: Diagram of the Retotype methodology.....	13
Figure 3: Architecture of the system	16
Figure 4: Biokey SDK Architecture.....	18
Figure 5: How user information is obtained.....	19
Figure 6: Main interface for server.....	20
Figure 7: Saving user's data.....	21
Figure 8: Complete capturing user's data.....	22
Figure 9: Verify success.....	23
Figure 10: Identification of the user.....	24
Figure 11: Identification failed.....	24
Figure 12: Flow of data to purchase a book.....	25
Figure 13: The main page of the website.....	26
Figure 14: Details of a book.....	27
Figure 15: GUI of fingerprint scanner application.....	28
Figure 16: Verification match.....	29
Figure 17: Identification failed message.....	30
Figure 18: Identification valid.....	30
Figure 19: Invalid user data.....	31
Figure 20: Form for purchasing the book.....	32
Figure 21: Status invalid.....	32

ABBREVIATIONS AND NOMENCLATURES

B2C	Business to Consumer
SSL	Secure Socket Layer
POS	Point of sale
ID	Identification
ROI	Return on investment
XML	Extensible markup language
XCBF	XML Common Biometric Format

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND OF STUDY

E-commerce has revolutionized the way of doing business. Rather than going to the shop to purchase a book, for example, a user would just use the Internet to buy it, and it is sent to the home.

Doing online transactions would need the user to enter their identification and also credit card number. This is where the risk takes place. There are many cases of fraud where people steal credit card numbers and guess passwords to gain access to purchase something online. Just with a few cases, the public's perception about e-commerce has already turned sour. This is why new ways are needed to gain back the trust of e-commerce users.

1.2 PROBLEM STATEMENT

In the era of globalization, numerous transactions are done each day. A person uses the Internet to buy goods, sell goods, do banking transaction and others. Everyone is moving from the hassle, into simple ways of doing daily chores. A person may not need to be physically there in the bookshop, to shop for a book, wait in queue and waste their time. Instead, a person may just sit in the comfort of his or her own home to purchase the book. E-commerce helps to make business grow. It does not bind the business to certain hours only, because it enables anyone from anywhere to access the website anytime.

The basic steps for customers to do transactions online are keying in their identification (ID), their password, and their credit card number. Assuming a thief could guess someone's ID, password and has in hand the credit card number, the thief could just purchase whatever he or she desires online, and does as many transactions he or she likes.

Customer credit card details and sensitive personal and company information are at widespread risk through simple e-commerce flaws, according to new research from Europe's leading full-service Internet security testing company, NTA Monitor. NTA Monitor's research into eCommerce flaws was conducted from October 2002 to January 2003, based on flaws commonly discovered during NTA's 'eCommerce Service' security assessments of authenticated web access and eCommerce systems.

CEO of Electracash, E. Lee Falls, a Long Beach California company that processes checks for e-merchants encountered one of the many flaws that lies in e-commerce. He handles payments for a chunk of the 20% of Web shoppers who choose not to put their credit-card numbers online every year. Electracash processed 1.2 million payments in 2002, and Falls says 5% to 10% of them came from cheaters and crooks. His problem, which lies at the root of e-commerce, is simple: Neither he nor anyone else can identify the person making a purchase on a distant computer. Passwords and PIN codes can be stolen, or even guessed.

Thus, other than Electracash, there are sure to be certain companies who are facing the same problem. A 5% lost may not look much, but accumulatively, if it affects 10 companies, the economy is losing 50% of the profit it may make if fraud does not happen. Hence, not only does this e-commerce flaw affects individual companies, but also it will affect the economy of the country overall.

Although a digital signature is another method that can be used to authenticate transaction, it is not a feasible method for this scenario. Digital signature is a method where the initiator (for example bank) would have two keys, which are public key and private key. The bank would give their customer a public key. By using this public

key, a user from the client side can send information to the bank (the information would be encrypted). The bank would receive the message and decrypt the message using the private key. Digital signature is not a feasible method, as it does not cater for large amount of users. For example, if the bank has 1,000,000 online customers, the bank would have to give its public key to all their customers. Thus, everybody would have the same public key. This method does not differentiate someone's uniqueness from another.

1.3 OBJECTIVES AND SCOPE OF STUDY

1.3.1 Objectives

The objectives of this project are to:

- produce a prototype, which uses biometrics as an authentication method during an online transaction.
- produce implementation strategies on the implementation of this system in the real world.

1.3.2 Scope of Study

The scopes of study for this project are:

- **fingerprint biometric**

Fingerprint biometric is used for this project rather than other biometric parts like iris scan. Generally, it is much easier to obtain the fingerprint scanner rather than iris scanner. Fingerprint biometric is a more common biometric than any other body parts. Is it also easier to handle, comparatively to voice recognition. A feasibility study of this technology will be derived from this project to show whether this technology is realistic enough to be implemented in the real world.

- **payment method using credit card**

This study is done to learn more how credit-card transaction works and how similar is it compared to biometric transactions.

- **B2C (business to consumer)**

The purpose of B2C study is to know how an e-commerce website works, and how it transacts from the client side to the server side. The client's end is usually the spot where e-commerce fraud happens. Thus, implementing fingerprint biometric at the front end is also relevant in making online transactions more secure. For this project, an online bookstore will be developed. Thus, the study of an online bookstore incorporating biometric is vital.

CHAPTER 2

LITERATURE REVIEW OR THEORY

2.1 THE E-COMMERCE PROCESS

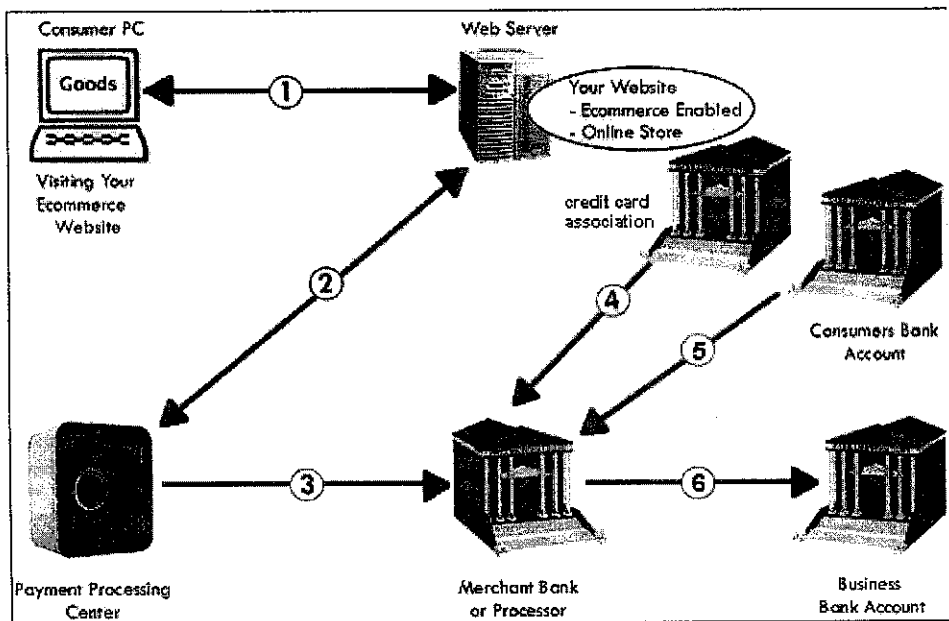


Figure 1: An online credit card transaction

Figure 1 shows how an online transaction using a credit card happens. This process usually takes place when a user purchases an item on the Internet. Below are the explanations for the process above:

- 1) A consumer visits an e-commerce website with an intention to purchase an item, for example Compact Disc. The transaction is conducted over a secure connection, Secure Socket Layer (SSL) to the web-hosting server. After selecting the desired item, the consumer would then fill up some information, to enable the item to be sent to the home.

- 2) Payment Processing Gateway would then handle the secure, real time encrypted credit card information and co-ordinates the transaction.
- 3) Merchant would obtain the information from the Payment Processing Center. The merchant bank would then process the movement of funds.
- 4) The information from the merchant bank would be transferred to the credit-card association from where the user got his or her credit card. Verification is then received from credit-card association to the merchant bank.
- 5) Funds are then debited from the consumer's credit card account.
- 6) Funds are then deposited into the company's designated bank account.

2.2 NUMBER ONE FRAUD IN E-COMMERCE

Identity theft occurs when an unscrupulous person gathers enough information about you to successfully impersonate you online, by mail, over the telephone, or in person, usually for criminal purposes. Identity theft ranked as the number one complaint in the United States of America. According to two studies done in July 2003 by Gartner Research and Harris Interactive, approximately 7 million people became victims of identity theft in the prior 12 months. That equals 19,178 per day, 799 per hour, and 13.3 per minute. About 107,500 people complaint about Internet-related fraud as scammers found victims through Web sites or spam e-mail, according to a Federal Trade Commission report.

Theft of personal information can be used to obtain new credit or services and new identification. In essence, the criminal assumes the victim's identity to take advantage of his or her established credit rating. Often the victim is unaware that the theft has occurred until they try to obtain new credit or they receive notification from collection agencies of unauthorized, yet outstanding, debt. This type of crime is devastating to the victim who is faced with trying to re-establish their rightful identity and credit rating. A connection between identity theft and organized crime groups has not been established.

Ansalleni (2003) reported that in the past five years identity theft crime category has boomed, and it now affects more than 27 million Americans. What's more, it costs businesses and financial institutions almost \$48 billion a year. As the incidence and financial damage of identity theft increases, so does the public's demand that policy makers enact new laws and regulations to stop this personal crime.

The Federal Trade Commission said it received more than half a million consumer complaints in 2003, as thief financed their spending sprees with other people's credit cards. Hence an online system that verifies a consumer's identity before processing transactions to prevent theft and fraud is needed so that only authorized user's transactions can be process. This can indeed reduce the cases of online fraud.

2.3 EFFECTS OF IDENTITY THEFT OR CREDIT CARD FRAUD

Online transactions do not take place at the point of sale (POS). They are considered to be "non-face-to-face" transactions. Since there is no way of ascertaining the customer's identification, there is no way to be sure that the customer is the legitimate card holder. Therefore, financial institutions are leery about the high potential for fraud.

Moreover, the major credit card companies offer their cardholders the right to contest charges on their statements that may be the result of theft, fraud or error. A contested charge is referred to as a chargeback. When a chargeback occurs, the merchant will end up paying the charge to the issuing bank, in addition to a chargeback fee that can be as high as \$30 or more in the United States. For example, if you sell a book for \$20 through a credit card transaction, and the cardholder later contests the sale; you will end up paying your bank the \$20 plus a chargeback fee of \$10 to \$30 dollars.

Consequently, many banks require a reserve fee when issuing merchant status. Typically, face-to-face sales have a chargeback rate of 1% of all sales. The potential

for chargeback's is greater when it is an online sale, so the risk to both bank and merchant increases.

2.4 DISADVANTAGES OF PASSWORD AUTHENTICATION

There are numerous disadvantages of using passwords. Passwords needed to belong in order to be secure. A password should be a mixture of alphabets, numbers and special characters. Thus, users will find it difficult to remember their password. A person password should be changed every three months to reduce the possibility of hackers guessing it. The users then tend to write them down somewhere, encouraging others to peep the password or they may loose the paper to an evil hand. Hence, passwords are easy to loose and easily forgotten. Someone might also be able to guess a person password, especially professional hackers. Thus, another alternative of doing e-commerce is needed to make transactions secure. While the password is very machine friendly, it is far from user-friendly.

2.5 BIOMETRIC AND WHAT IT DOES

Russell (1992) quoted that "Every person has a set of unique physiological, behavioral and morphological characteristics that can be examined and quantified" (p.246). Thus, biometric is the use of these characteristics to provide thrust-worthy personal identification. There are many types of biometric, which can be used as an identification instrument, namely fingerprint, retina pattern, handprint, voice pattern, keystroke pattern and signature. At the moment, only fingerprint, handprint and retina pattern system are properly classified as biometric systems as they actually test physical characteristics. Everybody has a unique set of characteristics, hence using biometric to identify someone is just a practical solution to password usage.

Biometric identification works like this: the identification system obtains data from the user, and then converts the analog data into digital representation. The digital representation is then compared to the “templates” stored in the system.

By using biometric, unauthorized access can be prevented, as the authorized party needs to be there to be able to verify the transaction made. For example, if a person has your credit card number and password, that person can purchase something online. But with biometrics, a password is not necessary. Although the person has your credit card number, the transaction cannot be completed, as your fingerprint scan is not available. Thus, this reduces anxiety among business people, as they fear of losing their password.

2.6 BIOMETRIC E-COMMERCE

The usage of biometric is very relevant in today’s world. People are so busy that they do not make an effort to remember passwords. Using fingerprint scan for e-commerce is a wise solution as the hardware is at the reasonable price. Many e-commerce website does not support this way of doing transaction as yet. Thus, the future of biometric in e-commerce may seem real, but yet far. Biggs (2004) states that by 2005, 60 percent of enterprise sites will continue to extend the use of ID and password constructs to ever more sensitive e-business applications. Gartner expects the impact of this extension to cause a rise in fraudulent accesses that will negatively impact the return on investment (ROI). Does this mean we should abandon ID and password constructs? Not at all. We just need to begin looking at ways to merge ID and password access with emerging authentication techniques. This will greatly reduce the threat of fraudulent accesses. Some of these include biometrics, digital signatures, smart card, and single sign-on” (*Fraud, negative ROI to lead businesses to embrace emerging biometric techniques*).

Surmacz (2004) reported that identity fraud and theft cost Americans at least \$437 million in 2003. Identity thefts numbered 215,000 reports, making a 33% increase

over the year before (*ID Theft Tops List of Costly Fraud Complaints*). According to the CyberSource Fraud 2000 Survey "...when (e-tailers were) asked to assess significant negative business impacts related to fraud, 29% mentioned the loss of customer goodwill, 23% charge backs, 22% loss of staff time, 18% loss of revenue, 12% loss of goods, and 8% bank fees." A Gartner survey of more than 160 companies revealed that 12 times more fraud exists on Internet transactions and those e-tailers are paying credit card discount rates that are 66 percent higher than traditional retailer fees.

As ever larger numbers of organizations start to transact business over the Internet and other open networks, it becomes increasingly important to achieve secure identity authentication.

2.7 BIOMTERICS ROLE IN SOLVING IDENTITY THEFT AND FRAUD

Chargebacks can be a real problem on the web since there is no signature and no imprint made when the users want to purchase a book. This makes it much easier to use bogus credit card numbers to perpetrate online fraud.

In addition to fraud perpetrated by thieves, there is also so-called "friendly fraud" which takes the form of customers who claim they did not purchase from you, even when they know they did.

Thus, to curb this rising problem, merchants should come up with a solution to ensure that this chargeback is reduced, hence increasing revenue. New technological ways, like fingerprint biometric can actually solve this real world problem. With fingerprint biometric, when a user wants to purchase a book, the user would need to scan his or her fingerprint. This fingerprint would then be the imprint as proof of purchase.

For example, a thief steals a person credit card number, and tries to purchase a Compact Disc online. With fingerprint scanning, the transaction would not be authenticated and verified by the merchant as the fingerprint of the thief will not

match with the owner of the credit card's fingerprint. This manner would indeed lower the risk of fraud from the merchant's perspective, hence increasing the revenue of the merchant company because there is no necessity to pay for chargeback fees.

To minimize their risks, most banks have stringent requirements that a business must meet to establish eligibility for merchant status. Factors considered include cash reserves, length of time in business, tax returns, credit history, debt load, refund policies, volume of business, cost of item being sold, and other sources of income.

2.8 PREVIOUS ONLINE BIOMETRIC WORKS

2.8.1 Using biometric for authenticating online exam students

Increasing interest in distance learning and assessment has lead to an increase in examinations being carried out using Internet based assessment. This has introduced a number of problem areas that need to be addressed so that reliable secure examinations can be carried out. The attraction of online examination comes from a number of sources; it offers advantages in time saving, as the candidate does not need to travel to an examining centre, this in turn removes the cost of travel and other related costs such as accommodation. Because the exam is computerized, the possibility for fully or partially automated grading and assessment exists. This can reduce costs further by removing the need for manual assessment and as a result offering quicker feedback of results and removes the possibility of human error during marking.

Unfortunately the inherent lack of a controlled environment at the candidate's end of a web-based link introduces a number of issues, mainly related to security. There are a wide range of products offering secure connection across the Internet that have been in place for some time and have been mainly proven as secure so issues with the assessment being tampered with in transit can be dealt with through the application of existing technologies. However methods of ensuring the authorized person is sitting at

the remote end of an Internet link are less secure and have been largely brushed under the carpet by organizations wishing to implement distance learning assessment, in fact very few papers exist on the subject. For a general login scenario the user will have a user name and associated password, offering a method of security acceptable for the majority of situations, in online examinations a number of interesting problems occur with this simple security procedure.

2.8.2 Biometric E-commerce

E-business standards consortium (OASIS) announced on March 7th 2002, that it has formed a committee to specify a standard way to use XML (extensible markup language) in biometrics for e-commerce and other applications. The new specification, called the XML Common Biometric Format (XCBF), will describe information that verifies identity based on human characteristics, such as DNA, fingerprints, iris scans and hand geometry. What is more, execution details are still largely undefined, according to analysts. A variety of housing devices for biometrics are still in the experimental stage, including smart cards, key chains and implanted computer chips. The problem may rise when consumers are charged with cost where per-user costs can reach US\$100, and expenses skyrocket for more sophisticated systems like iris scans.

CHAPTER 3

METHODOLOGY/PROJECT WORK

3.1 PROCEDURE IDENTIFICATION

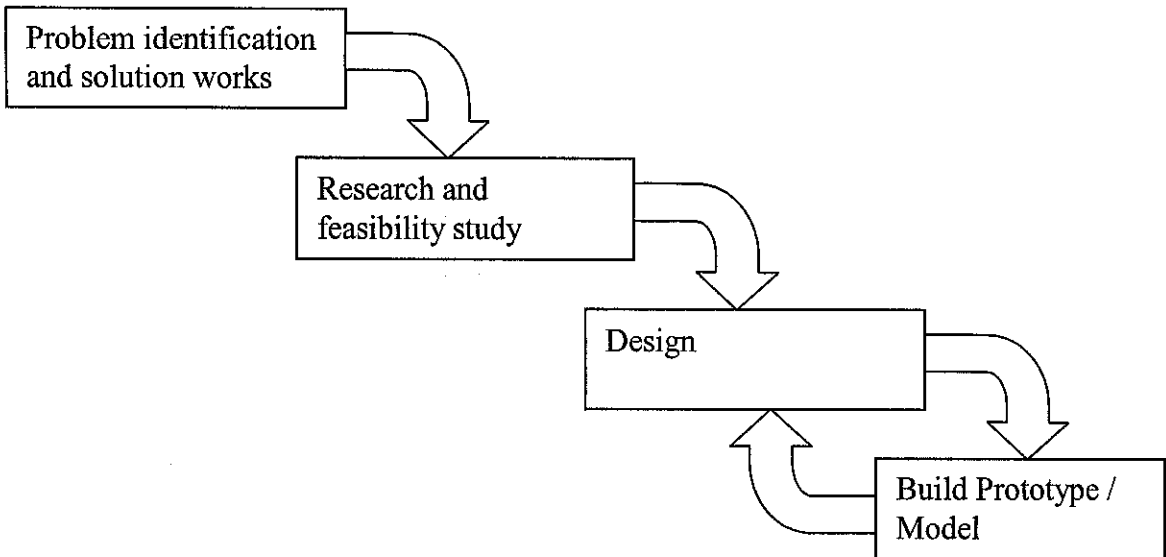


Figure 2: Diagram of the Retotype methodology

Retotype is a combination of research or information gathering and prototype. The following will explain in detail each process in order to complete this project.

3.1.1 Problem Identification and Solution Work

At the beginning stage, the problem definition is defined thoroughly. This project looks into e-commerce and how fingerprint biometric can be integrated into the e-commerce framework. E-commerce fraud can be lessening if this framework is feasible in the real world.

3.1.2 Research and Feasibility Study

Research was done by finding articles on the Internet, journals and also books from the library. Specific topics like biometric, e-commerce, B2C would be the main interest in this project. A thorough literature review is produced by using the materials found. With this literature reviews, it will guide the project towards the objectives set earlier. By going through this phase, it can evaluate whether fingerprint biometrics is suitable in the almost real world scenario.

3.1.3 Design

This design phase involves a detail and accurate design of an online bookstore website and the integration of fingerprint biometrics in it. It specifies the architecture of the website, the user interface and the biometric software. The website is designed using Macromedia Dreamweaver and ASP to process the forms filled by the consumer.

3.1.4 Build Prototype/ Model

A prototype of an e-commerce website will be built. The website will incorporate fingerprint biometric as a method of authentication. The fingerprint biometric will consist of a hardware and software, named Biokey. This hardware and software will reside at the merchant. The e-commerce website will reside at the client's end, where it communicates with the consumer. The hardware, software and the e-commerce website are integrated together by converting the Biokey SDK, which was developed using Visual Basic 6.0, into ActiveX Control. With this conversion, the Visual Basic application can be viewed and run in the Internet Browser and thus can be linked to the e-commerce website produced. Testing is performed after the completion of the prototype. These phases can also reiterate with the phase before it. Thus, design and testing will be done again and again until the system works.

3.2 TOOLS REQUIRED

3.2.1 Hardware

- Personal Computer with processing speed of 750MHz, 128 MB RAM and hard disk storage 1GB should be sufficient.
- Fingerprint scanner

3.2.2 Software

- Platform used is Windows 2000 Professional
- Visual Basic 6.0 – to alter the fingerprint scanner SDK.
- Biokey Software
- Microsoft Internet Information Server (IIS) 5.1
- Web authoring tool – Macromedia Dreamweaver

CHAPTER 4

RESULTS AND DISCUSSION

4.1 ARCHITECTURE OF BIOMETRIC E-COMMERCE

At the end of this project, a prototype is developed incorporating fingerprint scan technology in the e-commerce website. The prototype will be able to demonstrate how this biometric technology can be used while doing e-commerce transaction. The server side will contain the biometric software, which will store the fingerprint templates and on the client's side, it is an interface where users can purchase some items.

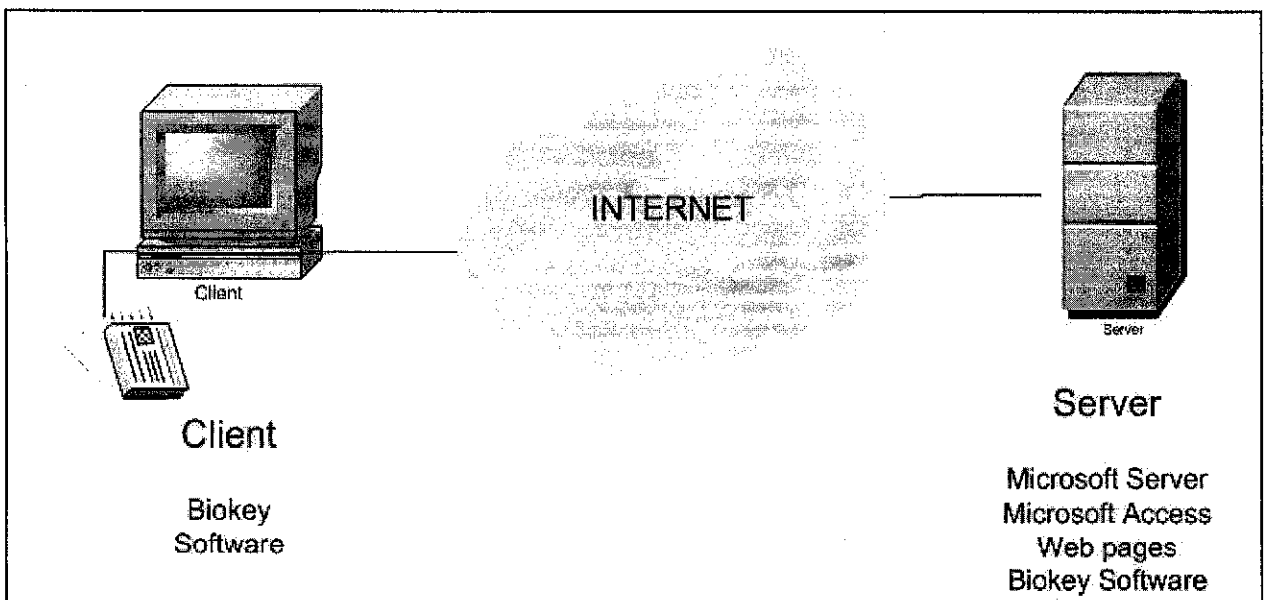


Figure 3: Architecture of the system

Figure 3 shows the architecture of the prototype. The figure includes the application that runs at each end of the architecture. The e-commerce website will be accessible at the client side and is kept at the server side, where it will also store the fingerprint database of the user. The fingerprint biometric reader is placed at the client's end as

depicted above. Whenever the client wants to purchase a book, the client would have to log into the website, select the desired book and fill in the forms. Before filling in the forms, the user at the client side would have to scan his or her fingerprint to authenticate and verify who he or she claims to be. After the scanning is done, and the authentication is verified, then only can the user fill in the form to order the book. After the user fills the form, the form is then sent to the merchant server. All other e-commerce process remains the same, as shown in Figure 3.

In this project, since the client and server reside on the same computer, thus it will not go through the Internet. Instead, it will be processed by the IIS installed in the computer.

4.2 BIOKEY ARCHITECTURE

Figure 4 shows the architecture of the Biokey SDK. This architecture is found in the hardware and software of Biokey. In order to be able to capture a user's fingerprint, there must be an application program at the front-end, which will interface with the user. When the fingerprint reader captures a fingerprint data, ActiveX Control OCX and device drivers will process the data and keeps the data in Microsoft Access. ActiveX Control OCX allows compound documents, which are data structures that contain different data types, such as text, audio files, and motion video files. The data would then be saved in the server, and used as comparison for authentication purposes.

The fingerprint scanner obtain is a USB port scanner. It is a quick and accurate 1:1 and 1:N fingerprint identification algorithm, which is effective and powerful for software developers and system integrators. This product can identify fingerprints from 2000 to 6000 pieces of fingerprints within 1-5 seconds (the following is tested on Pentium III 900MHz+ 128 MB EMS memories).

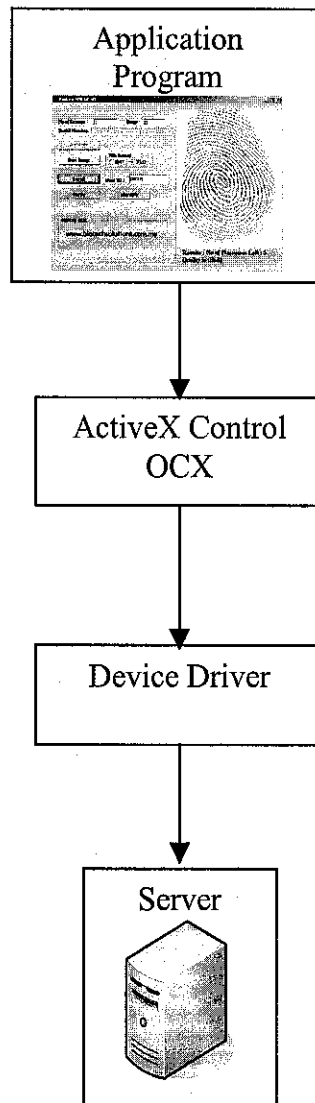


Figure 4: Biokey SDK Architecture

This device uses its Biokey algorithm, which is able to weaken noise, increase the contrast degree of the bridge and ridges, and to even capture whole or partial feature points from fingerprints of bad quality. The template size for each fingerprint is about 310 or 1152 Bytes only. The image quality scanned by the fingerprint scanner is approximately 300dpi. The false acceptance rate (FAR), which is the probability that a sample falsely matches the fingerprint template, is less than 0.001%. The false rejection rate (FRR), which is the probability that a sample of the right person is falsely rejected is less than 2.0%.

4.3 STAGES IN THIS SYSTEM

To enable a user to successfully purchase a book online, there are three stages that a user will go through, namely the 'Before', 'During' and 'After'.

The 'Before' stage takes place when the user registers himself or herself at the physical store. The 'During' stage takes place when the user surfs the website and is interested to purchase a book online. Finally, the 'After' stage is when the server receives the request from the user to purchase the book and process that transaction.

4.3.1 The 'BEFORE' Stage

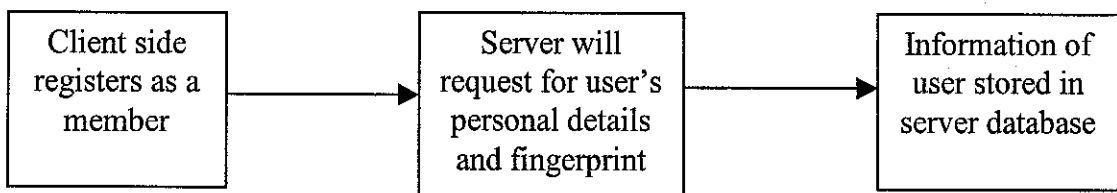


Figure 5: How user information is obtained

Figure 5 shows how the 'Before' stage is completed. The objective of this stage is to obtain user's information to be kept in the database. Firstly, the user would have to register as an online member with the physical store, at the shop's registration counter, to be able to purchase the book online. Each member who has registered will have to purchase an online fingerprint scanner. In this scenario, WISDOM Bookstore sells the fingerprint scanner hardware and drivers at a subsidized price compared to the market price. This hardware is customized by the store according to the store and e-commerce needs. Upon registration, the user would be asked to give their personal details and will be asked to scan their fingerprint. This information obtained from the user will be processed and stored at the server side (database).

The system at the server side is a stand-alone system. This process is done during the 'Before' to obtain user personal details and fingerprint.

The screenshot shows a web browser window titled "Wisdom Bookstore". The main content area contains a registration form with the following fields and controls:

- No of Sensors:** A text input field containing the value "1".
- Usage:** A text input field containing the value "0".
- Serial Number:** A text input field containing the value "{7C265690-0009-2002-0130-000000000249}".
- Initialize:** A button.
- Save Image:** A button.
- File format:** A section containing two radio buttons: ☒ **BMP** and ☐ **JPEG**.
- User ID:** A text input field containing the value "pennygo".
- Credit Card Number:** A text input field containing the value "276589012356".
- Enroll:** A button.
- Verify:** A button.
- Identify:** A button.

Below the form, there is a footer text: "Please Visit www.wisdom.com for more information. All Rights Reserved. InawadYou Production".

To the right of the form, there is a large, circular fingerprint scan image. Below the scan image, the text reads: "Results : No of Placement Left : 3" and "Quality is : Good".

Figure 6: Main interface for server

Figure 6 shows the main interface for the server. Upon registration at the physical shop, the bookshop attendant would request the user to key in their particulars as shown above. The user would have unique user identification. This identification name cannot be repetitive with other users. The main objective of this system is to reduce e-commerce fraud. Thus upon registration, the user would also have to give their credit card number. This is important because a registered user can have valid user identification, but uses other people's credit card number, to charge the credit to that account. The system then uses the user identification, credit card number and fingerprint data to compare with the database to verify the user's identity. After keying in the particulars, the shop attendant would click 'Enroll' to enroll the new user. The user's finger is then placed on the scanner for scanning. In Figure 6, it shows on the

right corner that 'Results: No of Placement Left: 3' and "Quality is: Good". When registering a new user, the number of times the user has to scan his or her finger is three times. This is done to allow the system to really capture and analyze the data. When the system shows "Quality is: Good", it shows that fingerprint captured is good enough to be stored in the database.

After scanning for three times, the system will pop-up a message as shown in Figure 7. If the attendant wants to save the data, the attendant would click 'Yes' and vice versa. After clicking 'Yes', the user has to scan his or her finger for the last time to verify the data.

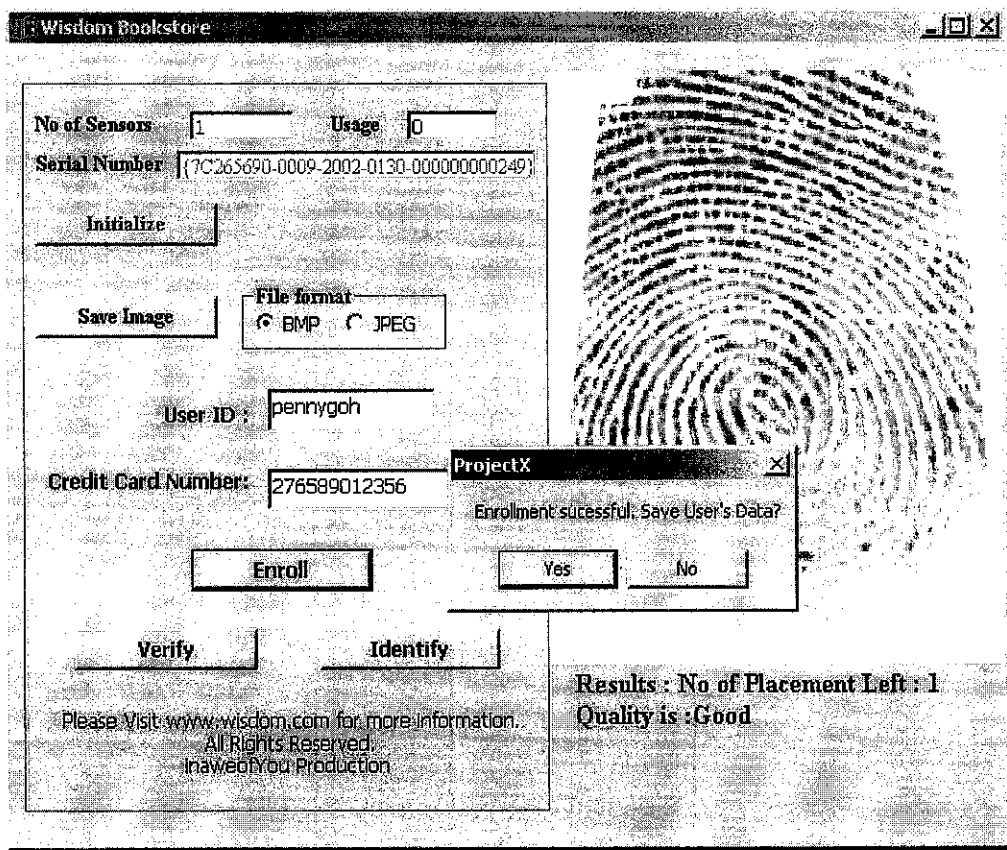


Figure 7: Saving user's data

The screenshot displays a web application window titled "Wisdom Bookstore". On the left is a form for capturing user data, and on the right is a large area for fingerprint capture.

Form Fields and Controls:

- No of Sensors:** Input field with value "1".
- Usage:** Input field with value "0".
- Serial Number:** Input field with value "{7C265690-0009-2002-0130-000000000249}".
- Buttons:** "Initialize", "Save Image", "Enroll", "Verify", and "Identify".
- File format:** Radio buttons for "BMP" (selected) and "JPEG".
- User ID:** Input field with value "pennygoh".
- Credit Card Number:** Input field with value "276589012356".

Fingerprint Capture Area:

- A large, circular fingerprint image is shown on the right side of the form.
- Below the image, the text "Capture Completed. (Place Finger)" is displayed.

Footer Text:

Please Visit www.wisdom.com for more information.
All Rights Reserved.
Inawedof You Production

Figure 8: Complete capturing user's data

Figure 8 shows that the user's data is completely captured and can be stored in the database. The attendant would have to click 'Verify' to verify the data. Once a message box as in Figure 9 appears, the data is already saved in the database. This data stored in the database (server) will be used as a comparison when users verify their information from the client side (web browser).

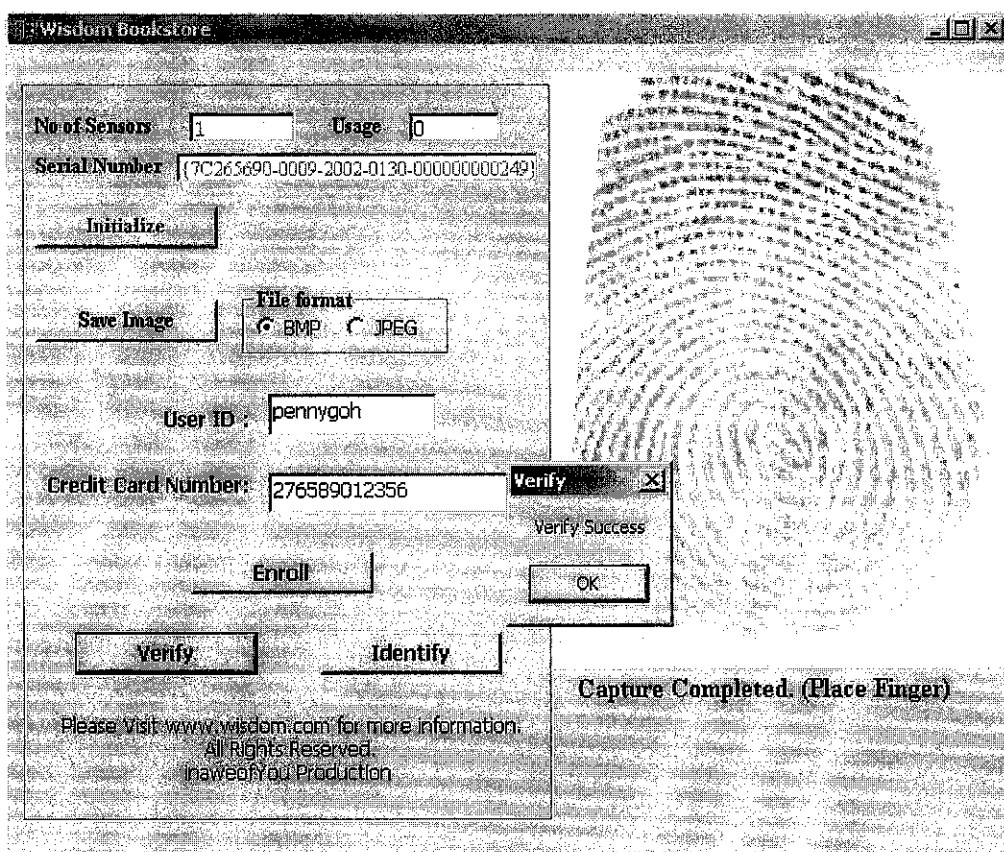


Figure 9: Verify success

The 'Identify' button allows a user to be identified. Firstly, the user clicks the 'Identify' button and then the user would place his or her finger on the fingerprint scanner to be scanned. After scanning, if the user were a registered member, a pop-up message as in Figure 10 would appear. This verifies that the user is a registered member of the bookshop. If the user is not registered in this system, the system will not be able to identify the user and will show an error as in Figure 11.

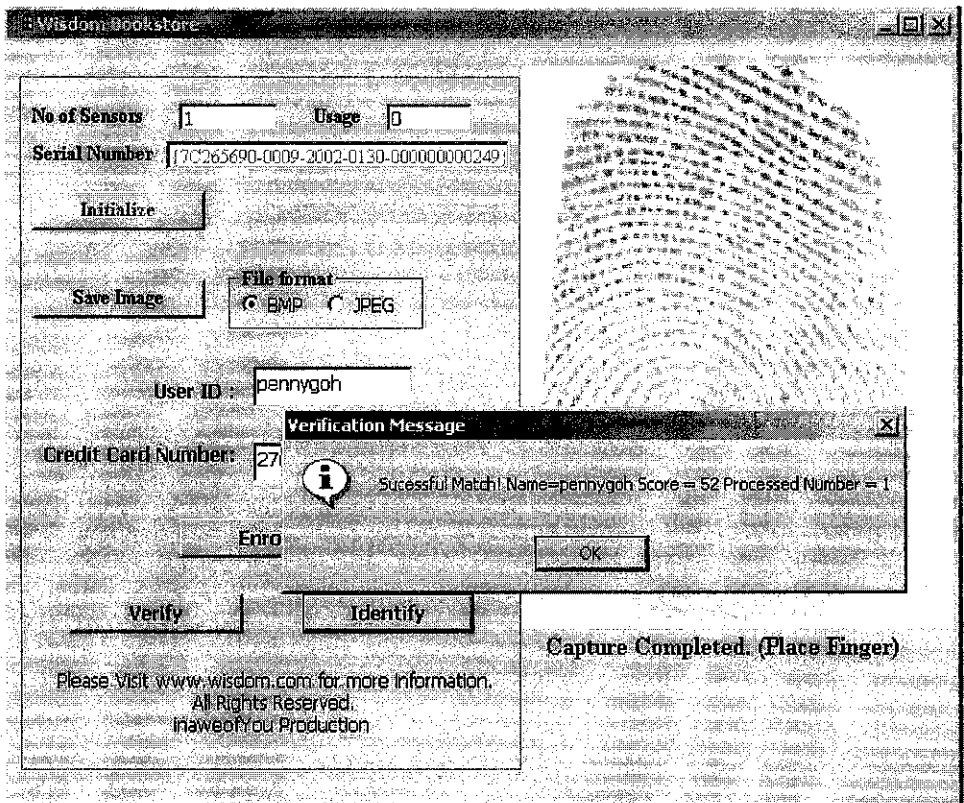


Figure 10: Identification of the user

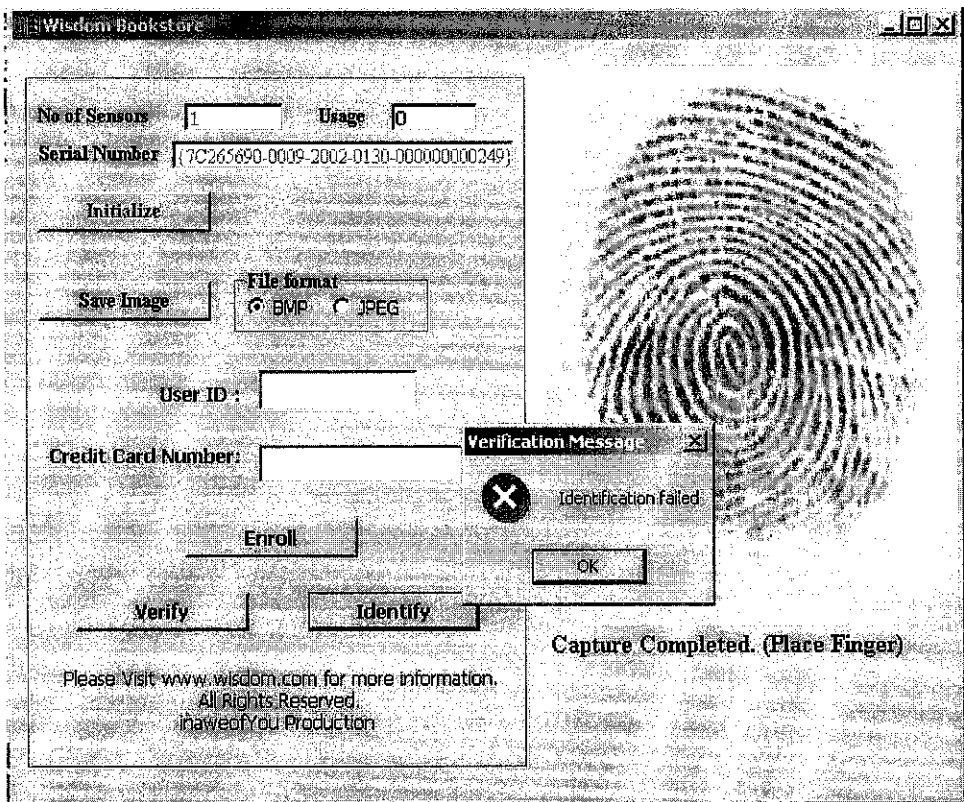


Figure 11: Identification failed

4.3.2 The 'DURING' Stage

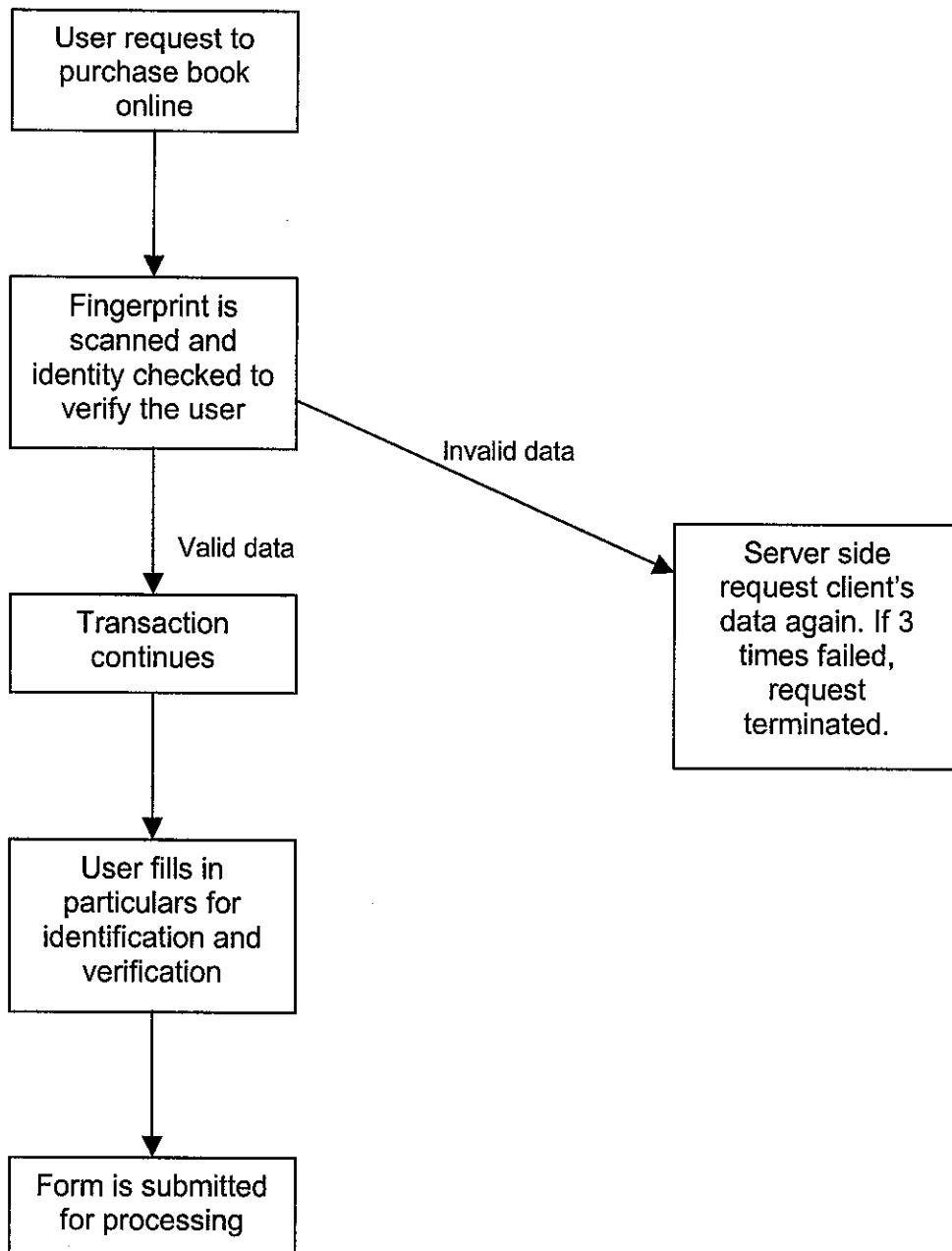


Figure 12: Flow of data to purchase a book

Figure 12 shows the flow of data when the user wants to purchase a book online. When the user at the client side wants to purchase a book, the user would then click the link "Click here to purchase!" (as can be seen in Figure 16) from the website. The

Biokey software in browser form will then load. The user would firstly press 'Verify' to scan their fingerprint and verify their identity. All other buttons and fields will be disabled. The fingerprint obtained will then be compared with the database at the server. If both the data matches, the user would key in their user identification (ID) and credit card number. The data would then be compared with the merchant's database. If the both the data matches, a new page would be displayed, requesting the user to key in personal details for the purchase of the book. If the fingerprint data does not match with the one at the server, the process would be terminated immediately, allowing the user to only browse the website. After the user fills in the particulars, the page would then be send to the server for processing. For prototype demonstration purpose, a personal computer will be used as a client, as well as a server. Internet Information Server would be the web server used at the server side.

4.3.3 Wisdom Bookstore Website

Figure 13 below shows the prototype of the e-commerce website built.

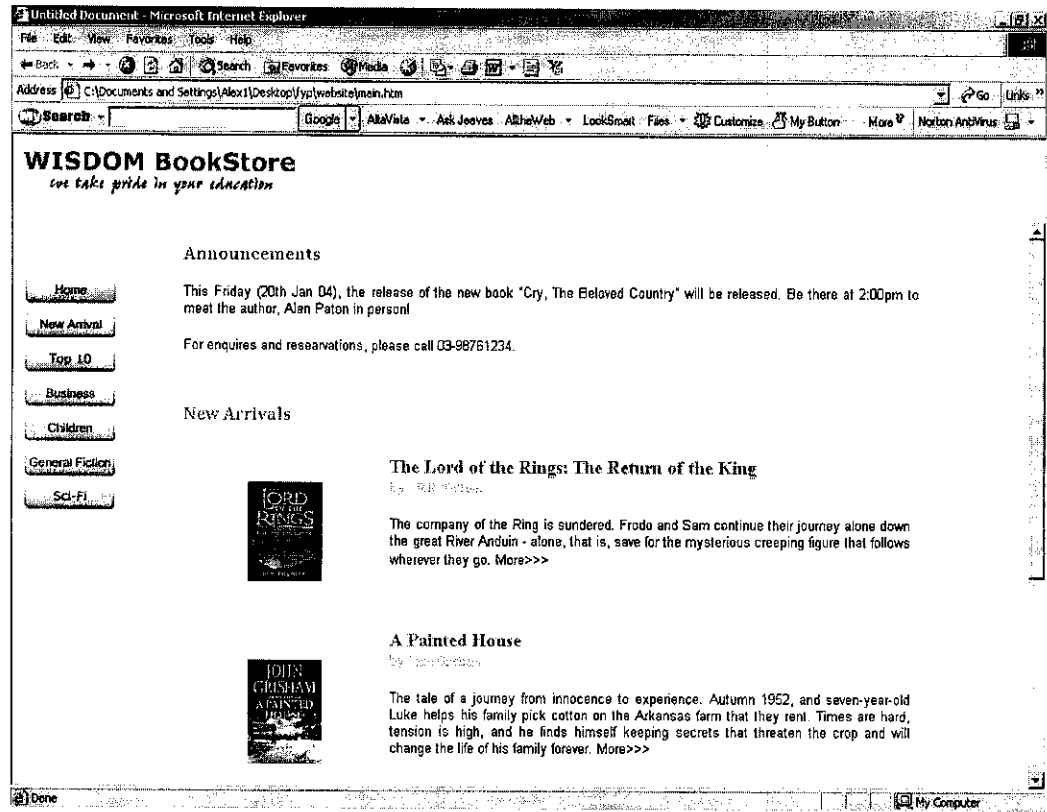


Figure 13: The main page of the website

This company name is known as Wisdom Bookstore, and it sells books online. The types of books that are available are fictions, children books and business books. As can be seen, the left side would consist of the menu and the right side would display the contents of each menu. If the user is interested to read in depth about a book, they may click on the link provided. Figure 14 would show the information of a particular book chosen.

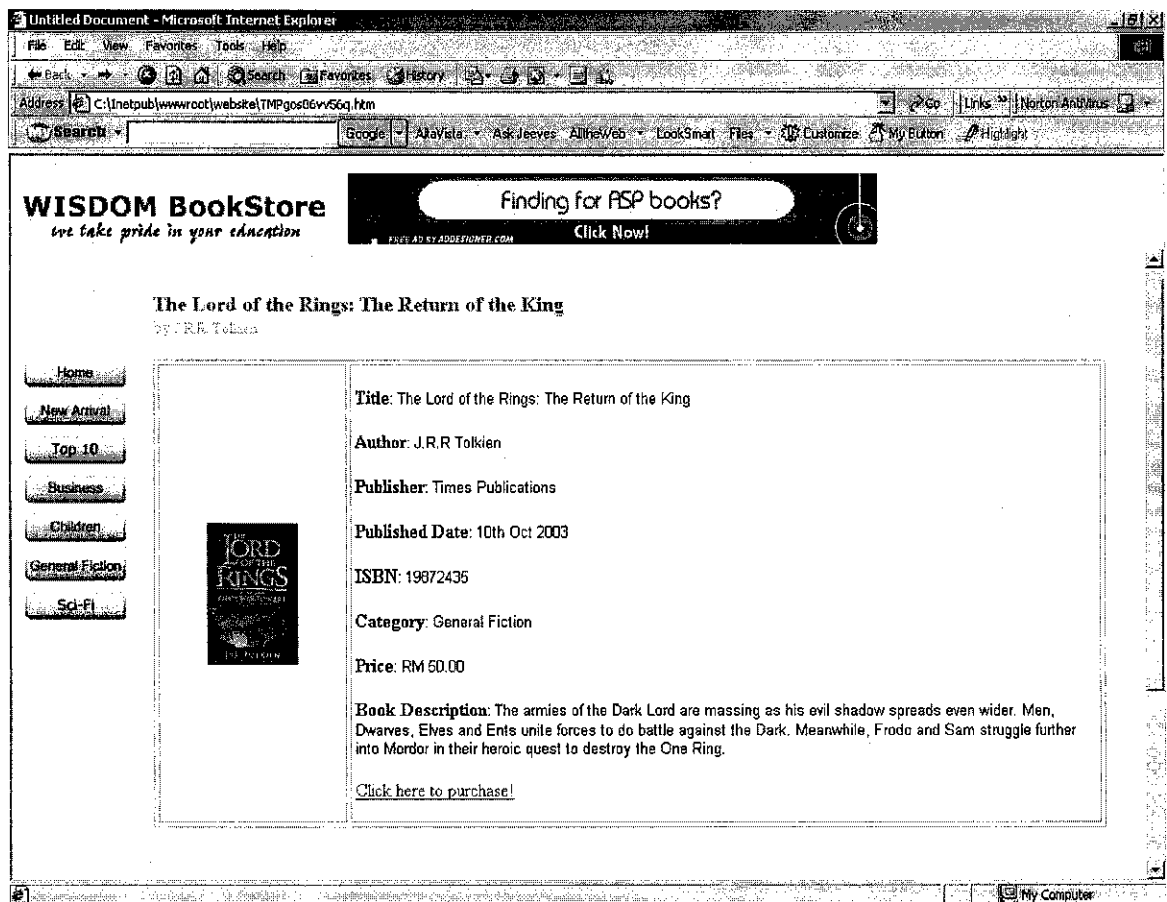


Figure 14: Details of a book

The page would display the information of the book and a little description about it. When the users click the link “Click here to purchase!” the consumer will then be directed to another page where the fingerprint biometric authentication takes place, as in Figure 15. Firstly, the user has to verify his or her identity. The user would have to

press the “Verify” button and scan his or her fingerprint. All other buttons and textboxes will be disabled.

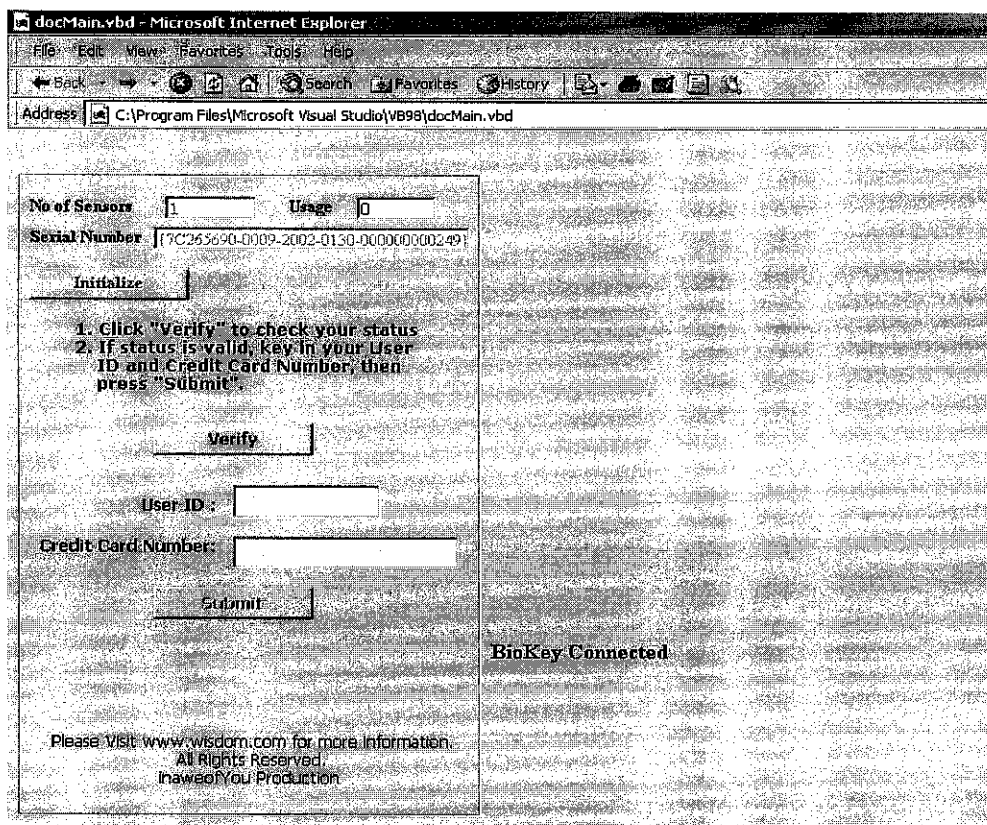


Figure 15: GUI of fingerprint scanner application

If identification is successful, Figure 16 will be shown. If the identification is unsuccessful, Figure 17 will show and will be directed to another page, as in Figure 21, to inform the user that he or she is not a register user yet. After the user’s identification is successful verified, the User ID and Credit Card Number fields will be filled. The user would then key in his or her identification, credit card number and press the ‘Submit’ button. If the information given by the user is valid, Figure 18 will show. The vice versa would be displayed as in Figure 19. If at anytime, during the verification process, the user is not a registered member, fills incorrect data to the verification form or trying to fake their identity, the transaction will be terminated, and the user will be directed to Figure 21, where the user can only view the website. Since all this process takes place at the client side, thus, the Biokey application is in web

based form. The Biokey application in Visual Basic is converted to web based using ActiveX Control. ActiveX Control is used because it allows Visual Basic application to be viewed in Internet browser.

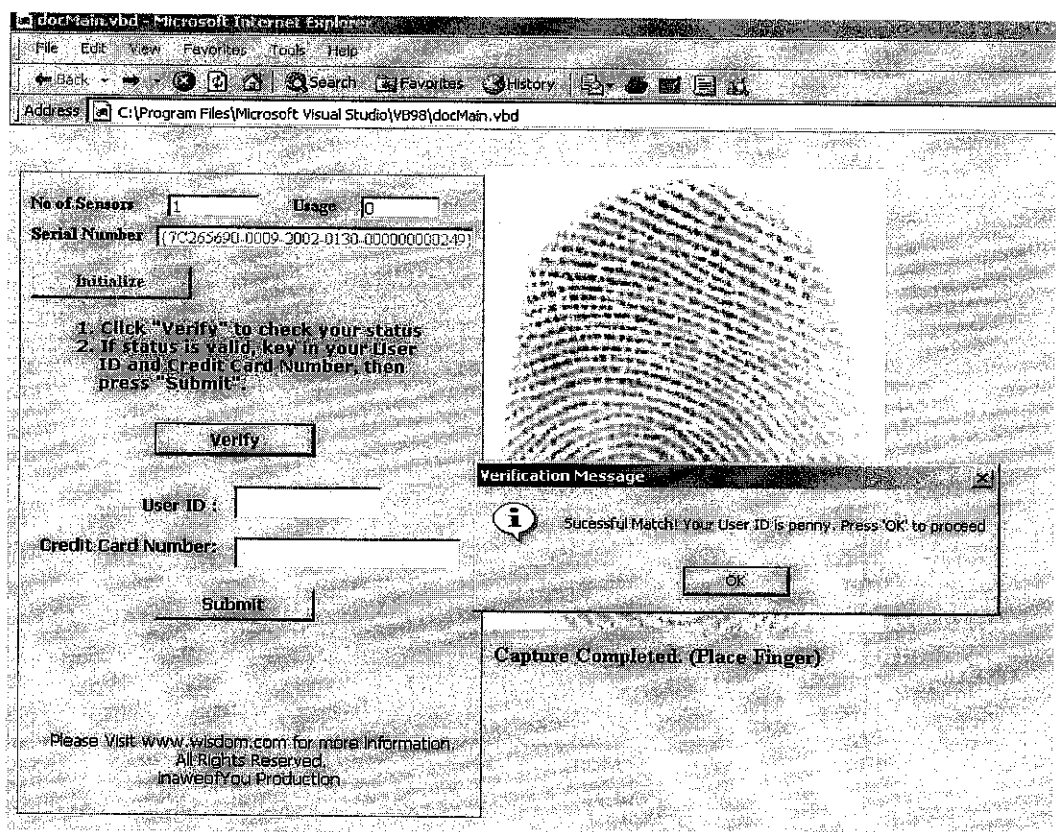


Figure 16: Verification match

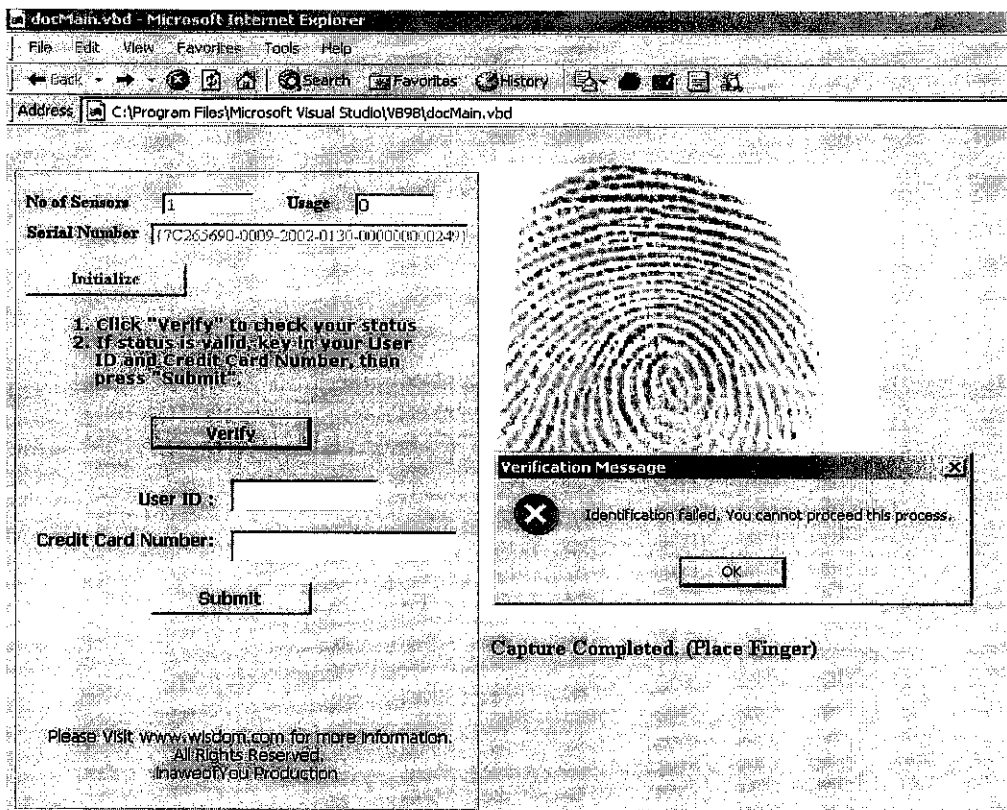


Figure 17: Identification failed message

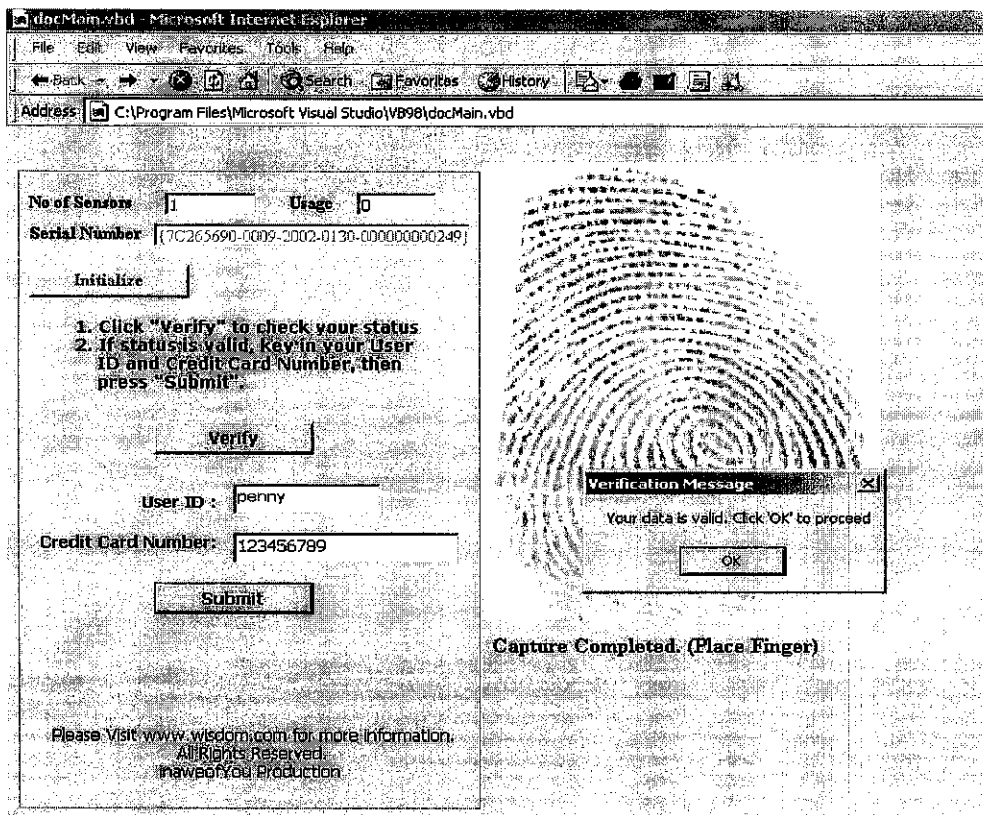


Figure 18: Identification valid

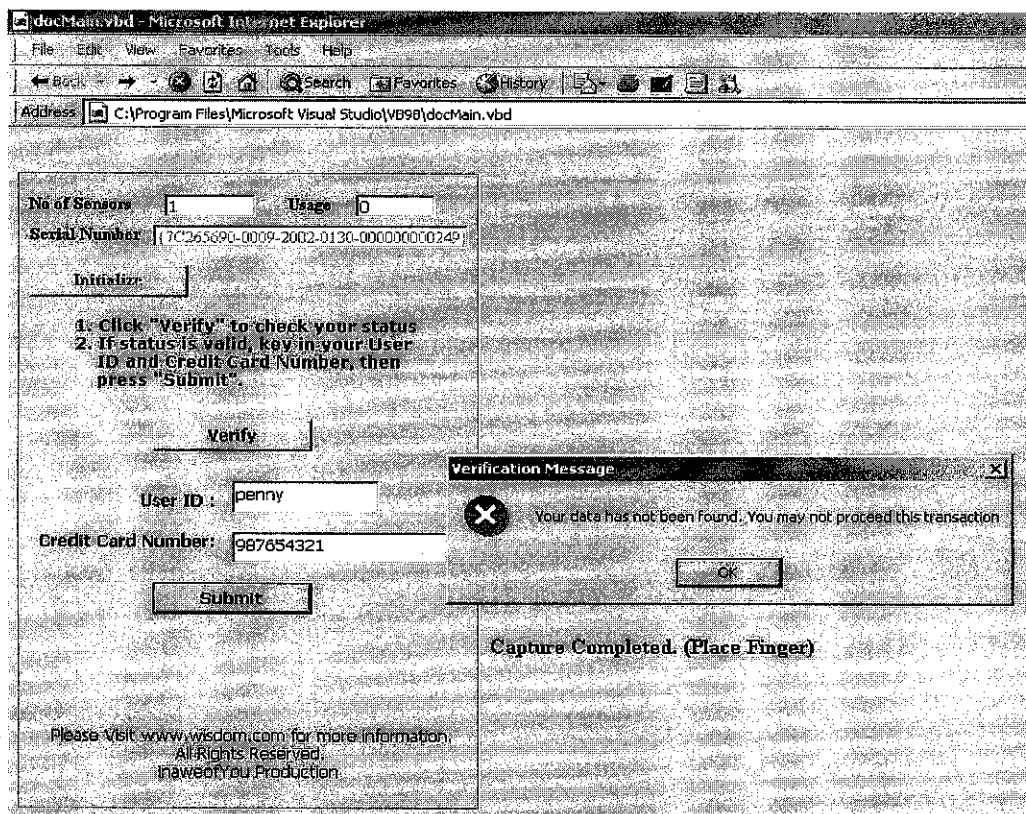


Figure 19: Invalid user data

After the verification process is done and valid, the transaction will continue, where the consumer would have to fill the forms including their personal details to be able to purchase the book. Figure 20 shows the form that the user will fill in.

Untitled Document - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address Go Links Norton Antivirus

WISDOM BookStore

we take pride in your education

Your status is verified. You may proceed by filling the form below.

The Lord of the Rings: The Return of the King
by J.R.R. Tolkien

You are making payment for the book above. Please fill in the details below:

[Home](#)
[New Arrival](#)
[Top 10](#)
[Business](#)
[Children](#)
[General Fiction](#)
[Sci-Fi](#)

Name :
 Address :
 City :
 Postcode :
 Country :
 Telephone :
 Credit Card Number :
 Type of Card :
 Expiration Date :
 Cardholder's Name :

Done My Computer

Figure 20: Form for purchasing the book

Untitled Document - Microsoft Internet Explorer

File Edit View Favorites Tools Help


Address Go Links Norton Antivirus

WISDOM BookStore

we take pride in your education

Your status is invalid. Please visit here to learn how to register with us. Thank You

[Home](#)

 Member's Day Sale

Done My Computer

Start Website 3:30 AM

Figure 21: Status invalid

4.3.4 The 'AFTER' Stage

The after stage happens when the information from the form that the users fill in leaves the client side personal computer and before it reaches the server side for processing. After the users complete the form to purchase a book, the form would then be submitted by the user to the merchant server for processing. Processing transactions securely on the web means that the transmitted information between the web site and the customer in a manner that makes it difficult for other people to intercept and read. SSL, or Secure Sockets Layer, takes care of this and it works through a combination of programs and encryption decryption routines that exist on the web-hosting computer and in browser programs used by the Internet public.

4.4 IMPLEMENTATION ISSUES

4.4.1 Implementation of biometric e-commerce

Consumer

There are two areas of concern when implementing biometric e-commerce in the real world for consumers, namely the cost of hardware and portability.

The cost of a fingerprint reader is RM285 for an equal quality as stated above. Since Wisdom Bookstore is subsidizing the cost, the bookstore sells it for RM150. This scanner would come along with software for installing the hardware drivers. The cost above may be expensive upon registration, but the online transaction that takes place is guaranteed secure. Furthermore, it reduces fraud and identity theft at the same time.

If a user has a laptop and brings it wherever the user goes, thus the software is already installed in the laptop, and the user only has to bring along the fingerprint scanner wherever. For instance, if the user is in Singapore and the user wants to purchase a book from Wisdom Bookstore online, the user has to bring along the fingerprint reader for authentication purposes. If the user has no laptop and is at outstation, the user

would then have to bring along the hardware and software wherever the user goes. The user would have to install the drivers on the computer he or she is using. This also applies if the user goes to the computer at the cybercafé if the user wants to purchase a book.

Merchant

A company that does e-commerce would be in favor of this new technology. Not only do the consumers benefit from fraud or identity theft, but the merchants can also reduce chargebacks and fake orders, thus increasing profit. Merchants who would like to implement this technology would have to change their current e-commerce website and incorporate fingerprint biometric into it. The merchants would also have to subsidize the cost of hardware and software for consumer as it is quite costly for the consumer to purchase it solely.

Fingerprint scanner vendors

Currently, the price of a fingerprint scanner is still costly. Not many people could afford to purchase one. If fingerprint reader for biometric e-commerce is a necessity in near future, everyone would demand for the hardware and software, and then the price of the reader would decrease. In the long run, all consumers would know the benefits of biometric e-commerce and the profit at the end would return to the vendors of the hardware and software.

4.4.2 Usage of biometric

Using biometric in e-commerce may be one of the many solutions in reducing online fraud and identity theft. Implementing biometrics must be practical to all types of users. There are some biometrics that can be implemented easily for online authentication, such as fingerprint, iris scan and signature recognition. Other kinds of biometric like voice recognition are difficult to implement as voice recognition is very abstract and varies. Iris scanner on the other hand is also expensive to purchase. Thus,

good usage of biometrics in different aspects will impact the effectiveness of a technology.

4.5 LIMITATIONS OF THE SYSTEM

4.5.1 Change of Credit Card Number

If the registered user wants to change his or her credit card number, the user is not able to change it online. The user would have to go to the physical bookstore to inform the attendant to make the necessary changes.

4.5.2 Security at server side

Another limitation of this system is that once the information from the client side travels through the secured network and reaches the merchant's server side; the information of the user from the client's side becomes vulnerable. Since the server is placed physically at the bookstore, any worker of the bookstore may open the database and view the user's confidential information. A worker may also obtain this confidential information and modify the information for personal benefits. Thus, no security measures are really taken at the server side.

4.6 FUTURE ENHANCEMENT

4.6.1 Scar finger

If for any reason a user's fingerprint that he or she register's with is not usable, the user will not be able to purchase a book online unless the user changes the fingerprint by going to the physical store. Thus, if the system is able to scan and store in the database two fingerprints at once, the user may still be able to purchase the book online even though one finger is injured.

4.6.2 Multiple credit cards

The system should also be able to store many credit card numbers at once. Thus, when the user wants to purchase a book online, the user may be allowed to choose which credit card he or she desires to use.

4.6.3 Change of credit card number

The website in the future enables the user to change their credit card number online. With this, the user does not need to go to the physical store to make changes. By using the fingerprint, the user is able to open their own database and make changes online.

CHAPTER 5

CONCLUSION

The purpose of this project was to see how a God-gifted trait can help people in technology. The use of biometric e-commerce is still new and much research is needed to make sure that implementation is successful. Biometric may not be the best solution to solve fraud or identity theft in e-commerce, but it is, at the moment, it can help in solving some of it. Through this project, a prototype incorporating biometric was developed. The conventional e-commerce architecture remains, but with the integration of fingerprint biometric, it will change the original architecture slightly. Most importantly, co-operation from all parties, for example, government and companies, is needed to make biometric e-commerce a success. There may be a slight change in the web design, and companies producing biometric hardware would have to price them slightly affordable for all. There are other traits of biometric that can be used, for example iris scan, voice recognition and others. Thus, much future enhancement is needed to be able to make biometric e-commerce favorable.

REFERENCES

1. Weidong Kou "Payment Technologies for E-Commerce" New York: Springer-Verlag Berlin Heidelberg, 2003.
2. Russell, Deborah, and Gangemi Sr. G.T "Computer Security Issues" New York: O'Reilly & Associates, 1991.
3. Ghosh A.K. "E-Commerce Security and Privacy" U.S.A.: Kluwer Academic, 2001.
4. Jain, Bolle, and Pankanti "BIOMETRICS: Personal Identification in Networked Society" U.S.A.: Kluwer Academic, 1998.
5. Ashbourn J. "Biometrics: Advanced Identity Verification" New York: Springer-Verlag Berlin Heidelberg, 2000.
6. "What are Identity Theft and Identity Fraud?" June 5, 2000. Mac 1, 2004
<<http://www.usdoj.gov/criminal/fraud/idtheft.html#What%20Are%20Identity%20Theft%20and%20Identity>>
7. "FTC says identity iheft, online fraud on the rise" January 22, 2004. Mac 1, 2004
<<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,89299,00.html?f=x10>>
8. "E-commerce Guide" No date. Mac 1, 2004
<<http://www.findmyhosting.com/ecommerce-web-hosting.htm>>

9. "Avoiding Chargebacks" No date. February 29, 2004
<<http://www.overdelivered-payment-processing.com/chargebacks.html>>
10. "Technology and Crime" June 2001. Mac 1, 2004
<<http://www.cisc.gc.ca/AnnualReport2001/Cisc2001/technology2001.html>>
11. "Committee Aims To Boost E-Commerce Biometrics" Mac 7, 2004
<<http://www.technewsworld.com/perl/story/16669.html>>
12. "Biometrics FAQ" 22 Mac 2004. Mac 15, 2004
<<http://www.bromba.com/faq/biofaq.htm>>
13. "Biometrics Solutions for Government and Industries" Mac 2004. Mac 15, 2004
<http://www.biometricgroup.com/government_and_industries.html>
14. "Fingerprint Biometrics in Network Applications" Jan 2001. Mac 17, 2004
<<http://www.eyenetwatch.com/fingerprint-recognition/biometrics.htm>>
15. "Fingerprint Biometrics" June 2001. Mac 24, 2004
<<http://www.eyenetwatch.com/fingerprint-recognition/biometrics.htm>>
16. "How fingerprint scanners work" Jan 2001. Mac 27 2004
<<http://computer.howstuffworks.com/fingerprint-scanner.htm>>
17. "Combining Biometric and Smartcard Authentication Modules" Feb 2003. April 1, 2004 <<http://www.caret.cam.ac.uk/projects/broniowski.htm>>